Hiding Traffic with Camouflage: Minimizing Message Delay in the Smart Grid under Jamming

Zhuo Lu Wenye Wang
Department of Electrical and Computer Engineering
North Carolina State University, Raleigh NC 27606
Emails: {zlu3, wwang}@ncsu.edu

Cliff Wang
Army Research Office
Research Triangle Park, NC 27709
Email: cliff.wang@us.army.mil

***Abstract*—The smart grid is an emerging cyber-physical system that integrates power infrastructures with information technologies. In the smart grid, wireless networks have been proposed for efficient communications. However, the jamming attack that broadcasts radio interference is a primary security threat to prevent the deployment of wireless networks. Hence, spread spectrum systems with jamming resilience must be adapted to the smart grid to secure wireless communications. There have been extensive works on designing spread spectrum schemes to achieve *feasible* communication under jamming attacks. Nevertheless, an open question in the smart grid is how to minimize message delay for *timely* communication in power applications. In this paper, we address this problem in a wireless network with spread spectrum systems for the smart grid. By defining a generic jamming process that characterizes a wide range of existing jamming models, we show that the worst-case message delay is a U-shaped function of network traffic load. This indicates that, interestingly, increasing a fair amount of redundant traffic, called *camouflage*, can improve the worst-case delay performance. We demonstrate via experiments that transmitting camouflage traffic can decrease the probability that a message is not delivered on time in order of magnitude for smart grid applications.**

I. Introduction

The smart grid is an emerging cyber-physical system that incorporates networked control mechanisms (e.g, advanced metering and demand response) into conventional power infrastructures [1]. To facilitate information delivery for such mechanisms, wireless networks that provide flexible and untethered network access have been proposed and designed for a variety of smart grid applications [2]–[4]. However, the use of wireless networks introduces potential security vulnerabilities due to the shared nature of wireless channels. It has been pointed out in [1], [2] that the jamming attack, which uses radio interference to disrupt wireless communications [5], [6], can result in network performance degradation and even denial-of-service in power applications, thereby being a primary security threat to prevent the deployment of wireless networks for the smart grid. How to defend against jamming attacks is of critical importance to secure wireless communications in the smart grid.

There have been extensive works on designing spread spectrum based communication schemes, which provide jamming resilience by using multiple orthogonal frequency or code channels [6], [7]. Interesting enough, most efforts attempt to design point-to-point or broadcast schemes such that a message *can* be sent to its destination. However, the key question to jamming-resilient communication for the smart grid is not whether a message can finally reach its destination, but whether it can be successfully delivered *on time* for time-critical power applications. For example, substation messages have 3ms–500ms delay constraints for reliable operation [8]. The over-due delivery of such messages directly results in communication failure, and can potentially lead to system instability [3], [9]. Therefore, an open question in the smart grid is *how to minimize message delay in spread spectrum based wireless networks under jamming attacks*.

In this paper, we address this issue by considering a wireless network that uses multiple frequency and code channels to provide jamming resilience for time-critical smart grid applications. As message delivery in the smart grid becomes invalid as long as its delay D is greater than the delay threshold σ, our goal is to minimize the message invalidation probability $\mathbb{P}(D>\sigma)$ in the presence of jamming attacks. A key observation in our approach is that there are two opposites in the network: the network operator and jammer attempt to minimize and maximize $\mathbb{P}(D>\sigma)$, respectively. As a result, we adopt a min-max approach to study the problem: i) find out which jamming attack can maximize $\mathbb{P}(D>\sigma)$ (e.g. the worst-case attack), ii) given the worst-case attack, attempt to minimize $\mathbb{P}(D>\sigma)$.

To find out the worst-case attack, we first define a generic jamming process that includes a wide range of existing jamming models. Then, we show via theoretical analysis that the worst-case delay performance is always induced by reactive jamming, which only sends jamming signals when it senses any transmission. Specifically, we find that under reactive jamming, the message invalidation probability is a U-shaped (first decreasing, then increasing) function of the network traffic load. This indicates that, interestingly, increasing a fair amount of redundant traffic (called *camouflage*) into the network can improve the delay performance for wireless smart grid applications under reactive jamming. Experiments show that camouflage traffic can decrease the message invalidation probability in order of magnitude, and thus it is a promising solution to combat reactive jamming for smart grid applications

The rest of this paper is organized as follows. In Section II, we introduce preliminaries and models. In Sections III and IV, we show camouflage traffic can minimize the worst-case

The work is sponsored by ARO under Grant Number 53435-CS-SR and NSF Career Award CNS-0546289.

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
MAR 2012		**00-00-2012 to 00-00-2012**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Hiding Traffic with Camouflage: Minimizing Message Delay in the Smart Grid under Jamming	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **North Carolina State University,Department of Electrical and Computer Engineering,Raleigh,NC,27606**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES
in Proceedings of the 31st Annual IEEE International Conference on Computer Communications (INFOCOM), Mini-Conference, 25-30 Mar 2012, Orlando, FL.

14. ABSTRACT
The smart grid is an emerging cyber-physical system that integrates power infrastructures with information technologies. In the smart grid, wireless networks have been proposed for efficient communications. However, the jamming attack that broadcasts radio interference is a primary security threat to prevent the deployment of wireless networks. Hence, spread spectrum systems with jamming resilience must be adapted to the smart grid to secure wireless communications. There have been extensive works on designing spread spectrum schemes to achieve feasible communication under jamming attacks. Nevertheless, an open question in the smart grid is how to minimize message delay for timely communication in power applications. In this paper, we address this problem in a wireless network with spread spectrum systems for the smart grid. By defining a generic jamming process that characterizes a wide range of existing jamming models, we show that the worst-case message delay is a U-shaped function of network traffic load. This indicates that interestingly, increasing a fair amount of redundant traffic, called camouflage, can improve the worst-case delay performance. We demonstrate via experiments that transmitting camouflage traffic can decrease the probability that a message is not delivered on time in order of magnitude for smart grid applications.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**Same as Report (SAR)**	**5**	

message delay. Finally, we conclude in Section V.

II. Models and Problem Formulation

In this section, we introduce network, communication and attack models, and then formulate the research problem.

A. Network Model

Wireless networks in the smart grid are in general used for local-area smart grid applications, such as substation automation and distributed energy management [3], [4]. Both frequency hopping spread spectrum (FHSS) and direct sequence spread spectrum (DSSS) have been proposed to be used in such networks to combat potential jamming attacks [3], [10]. Thus, in this paper, we consider a wireless local-area network $\mathcal{N}(m, N_f, N_c)$ for local-area smart grid applications, where m is the number of nodes in the network, N_f and N_c are the numbers of frequency and code channels, respectively.

In local-area smart grid applications, a large amount of network traffic features a constant traffic model for continuous monitoring and control of power equipments [3], [8], [9]. In addition, nodes can have distinct network traffic loads for different applications. For example, merging-units in a substation can send data of sampled power signal quality at various rates of 960–4800 messages/second, dependent on configuration [9].

Thus, we assume that there are heterogeneous traffic loads in network $\mathcal{N}(m, N_f, N_c)$; i.e., node i has a constant traffic load of λ_i messages/second ($i \in \{1, 2, \cdots, m\}$) in the network.

B. Communication and Interference Models

In the smart grid, to ensure in-time monitoring and control of power devices, a large amount of communication messages have stringent timing requirements. For example, substation applications have 3ms–500ms delay constraints for message delivery [8]. We refer to such messages as *time-critical* messages. The nature of time-critical messages indicates that they should be immediately transmitted and avoid being buffered. For example, time-critical messaging in substation communications [8] features a simple transmission mechanism at the application layer: bypass TCP and retransmit the same message multiple times to ensure timely delivery and reliability. Thus, we also adopt such a mechanism at the application layer of each node.

When a message is passed from the application layer to the MAC layer, traditionally, CSMA/CA is used to sense the channel activity before sending the message. However, CSMA/CA is primarily designed for one-channel networks, and may not be efficient in spread spectrum systems. In network $\mathcal{N}(m, N_f, N_c)$, the wireless channel is separated into N_f frequency and N_c code channels. Such channels can be considered orthogonal to each other. Even if there are multiple wireless transmissions over the same frequency channel, they will be successfully decoded at receivers as long as they use distinct code channels. CSMA/CA, which defers a transmission after sensing any activity on a frequency channel, may unintentionally degrade the delay performance.

As a result, we assume that when the MAC layer receives a message, it will directly transmit the message on a frequency-code channel pair, the (i, j)-th channel. Since the application layer will retransmit the message multiple times, the MAC layer will assign a different frequency-code channel to each retransmission. The assignment is a secret key known only to the sender and receiver. In addition, we assume that for a sender-receiver pair, each channel assignment is uniformly distributed over all $N_f N_c$ channels such that the chance of channel collision among legitimate nodes can be minimized.

We assume that the message transmission on the (i, j)-th channel fails only if at least a portion ρ ($0 < \rho < 1$) of the transmission is disrupted by jamming or collides with other legitimate traffic on the same (i, j)-th channel. In other words, we assume that the transmission of a message with a bits on a channel fails as long as at least ρa bits are corrupted.

C. Generic Jamming Model

The objective of a jammer is to broadcast radio interference to disrupt message delivery in network $\mathcal{N}(m, N_f, N_c)$. We assume that the jammer has the knowledge of the pools of frequency and code channels. However, it does not know what assignments are used by nodes to communicate with each other in that nodes can periodically use on-line jamming-resilient protocols (e.g., [6], [7]) to update secret keys. As network $\mathcal{N}(m, N_f, N_c)$ has multiple channels, the jammer can adopt a wide range of strategies to disrupt message delivery. There are two major jamming types in the literature: non-reactive and reactive models [5]–[7]. Non-reactive jammers transmit radio interference by following their own strategies. Reactive jammers transmit interference only when they sense any activity on a wireless channel. As we attempt to find out the worst-case attack, we define a generic process to accommodate both non-reactive and reactive jamming models.

Definition 1 (Generic Jamming Process): A jammer's jamming process is denoted as a Markov-renewal process

$$((F, C), X) = \{(F_k, C_k), X_k | k = 1, 2, \cdots\},$$

where (F_k, C_k) is the k-th state denoting a targeted frequency-code channel pair, X_k is the renewal interval denoting the k-th jamming duration on a channel. The embedded transition matrices associated with states (F_k, C_k) are denoted as $\mathbf{Q}_f$ and $\mathbf{Q}_c$, respectively. When the jamming is non-reactive, $((F, C), X)$ is a continuous Markov process, i.e., the renewal interval X_k is exponentially distributed. When the jamming is reactive, $X_k = \tau + S_k \mathbf{1}_A$[1], where τ is the constant sensing time for a channel, S_k is the duration of the jamming signal, A denotes the event that a channel is sensed busy.

As we can see in the Markov-renewal model, $\{X_k\}$ and $\{(F_k, C_k)\}$ can directly reflect when a certain channel is affected by the jamming attack, and matrices $\mathbf{Q}_f$ and $\mathbf{Q}_c$ can model what the jamming strategy is.

[1] $\mathbf{1}_A$ denotes the indicator function, which have the value 1 for A and the value 0 for A^c.

D. Problem Formulation

The primary goal of smart grid communication is to achieve timely management of power applications. Therefore, the delay performance is of critical importance. A time-critical message becomes invalid as long as its message delay D is greater than its delay constraint σ. As a result, we focus on how to minimize the message invalidation probability $\mathbb{P}(D>\sigma)$ under the generic jamming process $((F,C),X)$.

As there are two opposites in the network: the network operator and the jammer attempts to minimize and maximize the message delay, respectively. The lowest bound of the message delay is always achieved when there exists no jammer or a naive jammer. From the perspective of security design, it is reasonable to assume that the network can possibly face the worst-case attack. Thus, we adopt a min-max approach to study the problem of minimizing message delay in the smart grid under jamming attacks: i) in a wireless local-area network $\mathcal{N}(m,N_f,N_c)$, for a time-critical application with delay threshold σ, what is the maximum impact of the generic jamming process $((F,C),X)$ on the delay performance $\mathbb{P}(D>\sigma)$; ii) given the worst-case scenario in Step 1, how to minimize $\mathbb{P}(D>\sigma)$.

III. Theoretical Analysis

In this section, we use the min-max approach to analyze the worst-case message delay under the generic jamming process.

A. The Impact of Jamming Attacks

Our first goal is to find the jamming attack that maximizes $\mathbb{P}(D>\sigma)$ in the network. As our generic jamming process characterizes both non-reactive and reactive jammers with distinct behaviors, we provide analytical results of their impacts on $\mathbb{P}(D>\sigma)$, respectively. We first present the results on reactive jamming.

Lemma 1 (Reactive Jamming): In a wireless local-area network $\mathcal{N}(m,N_f,N_c)$ under a reactive jamming process $\{(F,C),X\}$ with sensing time τ, for a time-critical application at node k, the message delay D_k satisfies

$$\mathbb{P}(D_k>\sigma)\leq\left(1-\left(1-\frac{1}{N_fN_c}\right)^{T_L(1-\rho)\gamma_k}\left(1-\frac{T_L}{\frac{\tau N_fN_c}{1-\rho}+\rho T_L^2\gamma_k}\right)\right)^{\sigma/T_L}, \tag{1}$$

for N_fN_c sufficiently large, where T_L is the message transmission duration, σ is the message delay threshold, $\gamma_k=\sum_{j=1,j\neq k}^{m}\lambda_j$, and λ_j is the traffic rate at node j.

Proof: Without loss of generality, assume that node 1 is transmitting a message with delay threshold σ. Each transmission has a duration of T_L. The application layer can transmit the message at most σ/T_L times. The i-th transmission attempt uses the (u_i,v_i)-th channel ($1\leq i\leq\sigma/T_L$).

The message invalidation probability $\mathbb{P}(D_1>\sigma)$ is equal to the probability that all σ/T_L transmission attempts are disrupted by either collision or jamming, i.e.,

$$\mathbb{P}(D_1>\sigma)=\mathbb{P}\left(\bigcap_{i=1}^{\sigma/T_L}(J_i\cup C_i)\right), \tag{2}$$

where C_i and J_i denote the events that the i-th transmission is disrupted by collision and jamming, respectively.

First, we derive the collision probability $\mathbb{P}(C_i)$. Since all nodes have constant traffic rates, during node 1's i-th transmission duration, there are $(1-\rho)T_L\sum_{j=2}^{m}\lambda_j$ transmissions at other nodes that can possibly collide with the i-th transmission. As the frequency-code channel for each transmission in the network is uniformly assigned among all N_fN_c selections, the collision probability is equal to the probability that there is at least one other transmission colliding with node 1's i-th transmission, which can be written as

$$\mathbb{P}(C_i)=1-(1-1/(N_fN_c))^{(1-\rho)T_L\gamma_1}, \tag{3}$$

where $\gamma_1=\sum_{j=2}^{m}\lambda_j$.

Then, we compute the jamming probability $\mathbb{P}(J_i)$. For the sake of simplicity, assume that the i-th transmission starts at time 0. Define a renewal process $N_i(t)=\sup_{n\in\{0,1,2,\ldots\}}\{\sum_{l=1}^{n}X_l<t\}$. Then $X_1,X_2,\cdots,X_{N_i(t)}$ are renewal intervals during period $[0,\ t]$, and $X_l=\tau+S_l\mathbf{1}_A$, where A denotes the event that a channel is sensed with activity, and S_l is the jamming duration.

To maximize its damage to the network, the reactive jammer should always set the jamming duration S_l to be ρT_L. This means that when the jammer senses a transmission, it always chooses the minimum effective jamming duration to disrupt the transmission such that it can immediately move on to sense and jam other channels. Thus, we choose $S_l=\rho T_L$.

In order to successfully disrupt the i-th transmission (e.g., J_i holds), the reactive jammer must switch to the (u_i,v_i)-th channel at least once during $[0,(1-\rho)T_L-\tau]$. Let event $B_l=\{\{F_l=u_i\}\cap\{C_l=v_i\}\}$. Then, we have

$$\begin{aligned}\mathbb{P}(J_1|u_i,v_i)&=\mathbb{P}\left(\text{at least one event holds in }\{B_l\}\right)\\&=\mathbb{P}\left(\sum_{l=1}^{N_i((1-\rho)T_L-\tau}\mathbf{1}_{B_l}\geq 1\right)\leq\mathbb{E}\left(\sum_{l=1}^{N_i((1-\rho)T_L-\tau}\mathbf{1}_{B_l}\right)\\&=E(N_i((1-\rho)T_L-\tau))\mathbb{P}(B_l)\\&=E(N_i((1-\rho)T_L-\tau))\mathbb{P}(F_l=u_i,C_l=v_i)\\&=E(N_i((1-\rho)T_L-\tau))/(N_fN_c),\end{aligned}$$

where the first inequality follows from Markov's inequality, and the third equality follows from Wald's equation. We then have

$$\begin{aligned}\mathbb{P}(J_1)&=\sum_{i=1}^{N_c}\sum_{j=1}^{N_f}E(N_i((1-\rho)T_L-\tau))/(N_fN_c)^2\\&=E(N_i((1-\rho)T_L-\tau))/(N_fN_c).\end{aligned} \tag{4}$$

To obtain $\mathbb{E}(N_i((1-\rho)T_L-\tau)$, we first have from the elementary renewal theorem

$$\lim_{t\to\infty}\mathbb{E}(N_i(t))/t=1/\mathbb{E}(X_l), \tag{5}$$

where $\mathbb{E}(X_l)=\tau+\rho T_L\mathbb{P}(A)$, $\mathbb{P}(A)$ is the probability that a channel is sensed busy and $\mathbb{P}(A)=1-(1-1/(N_fN_c))^{(1-\rho)T_L\gamma_1}$. Then, it is reasonable to assume that the sensing time $\tau\ll T_L$ and the average renewal interval $\mathbb{E}(X_l)\ll T_L$ since power networks should always have unsaturated traffic loads [3], [8]

for timely monitoring and control. Thus, it follows that

$$\mathbb{E}(N_i((1-\rho)T_L-\tau)) \approx \frac{(1-\rho)T_L-\tau}{\mathbb{E}(X_l)} \approx \frac{(1-\rho)T_L}{\mathbb{E}(X_l)}$$
$$=\frac{(1-\rho)T_L}{\tau+\rho T_L-\rho T_L\left(1-\frac{1}{N_fN_c}\right)^{(1-\rho)T_L\gamma_1}} \approx \frac{(1-\rho)T_L}{\tau+\frac{\rho(1-\rho)T_L\gamma_1}{N_fN_c}}. \quad (6)$$

The last approximation follows from the fact that $(1-x)^a \approx 1-ax$ for small x. From (4) and (6), we obtain

$$\mathbb{P}(J_i) \le \frac{(1-\rho)T_L}{\tau N_fN_c+\rho(1-\rho)T_L^2\gamma_1}. \quad (7)$$

Finally, combining (2), (3) and (7) completes the proof. □

Next, we present our results on non-reactive jamming.

Lemma 2 (Non-Reactive Jamming): In a wireless local-area network $\mathcal{N}(m, N_f, N_c)$ with a non-reactive jamming process $\{(F, C), X\}$, the message delay D_k of a time-critical application at node k satisfies

$$\mathbb{P}(D_k>\sigma)\le\left(1-\left(1-\frac{1}{N_fN_c}\right)^{T_L(1-\rho)\gamma_k}\left(1-\frac{1-\rho}{e\rho N_fN_c}\right)\right)^{\sigma/T_L}, \quad (8)$$

where T_L is the message transmission duration, σ is the message delay threshold, $\gamma_k = \sum_{j=1,j\neq k}^{m}\lambda_j$, and λ_j is the traffic rate at node j.

Proof: We use the similar technique in renewal theory to prove Lemma 2. We omit details due to the page limit. □

Based on Lemmas 1 and 2, we show in the following that reactive jamming in general leads to the worst-case delay performance, thereby maximizing the damage to the network.

Theorem 1 (Worst-Case Delay Performance): For a wireless local-area network $\mathcal{N}(m, N_f, N_c)$ with sufficiently large N_fN_c, the worst-case delay performance at node k is always induced by the reactive jamming, and its message delay D_k is bounded by (1).

Proof: Comparing with (8) and (1), it suffices to show

$$\frac{(1-\rho)T_L}{\tau N_fN_c+\rho(1-\rho)T_L^2\gamma_k} \ge \frac{1-\rho}{e\rho N_fN_c}, \quad (9)$$

which is equivalent to

$$\tau \le e\rho T_L - \rho(1-\rho)T_L^2\gamma_k/(N_fN_c) \quad (10)$$

For N_fN_c sufficiently large, $\rho(1-\rho)T_L^2\gamma_k/(N_fN_c) \approx 0$. Then, since $e \approx 2.718$ and $\tau \le \rho T_L$ (the sensing time is smaller than the minimum jamming duration), it always holds that $\tau \le e\rho T_L$, which completes the proof. □

Remark 1: In practice, spread spectrum systems should always have large N_f or N_c to effectively combat jamming attacks. Thus, Theorem 1 shows that reactive jamming is more harmful than non-reactive jamming in wireless networks for the smart grid. From the perspective of security design for the smart grid, it is reasonable to consider reactive jamming as the worst-case scenario for smart grid applications.

Example 1: Fig. 1 shows an example of the worst-case message invalidation probabilities induced by both non-reactive (8) and reactive jamming (1) for time-critical applications at node k. We can see that reactive jamming always leads to worse delay performance than non-reactive jamming, and that

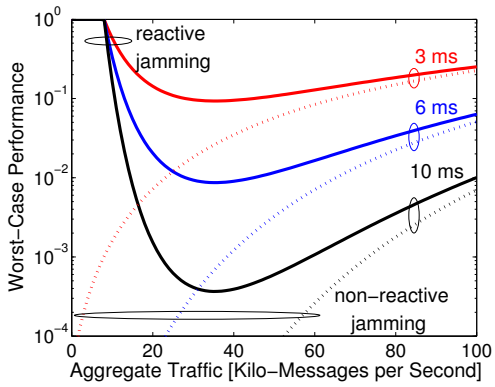

Fig. 1. Worst-case delay performance $\mathbb{P}(D_k > \sigma)$ versus aggregate traffic γ_k at node k for time-critical applications with delay thresholds of 3–10ms. (N_f=N_c=10, T_L=1ms, ρ=0.1, and τ=100μs for reactive jamming)

the delay performance at node k also depends on the aggregate traffic load γ_k. An interesting observation from Fig. 1 is that in the reactive-jamming case, the message invalidation probability is not minimized at γ_k^*=0. Instead, it is minimized at a fairly large value $\gamma_k^* \approx 38$ kilo-messages/second.

Remark 2: Fig. 1 illustrates that, interestingly, the worst-case delay (caused by reactive jamming) is in fact a U-shaped (first-decreasing then-increasing) function of traffic load γ_k. This is due to the sensing and reacting nature of reactive jamming. Intuitively, when there is redundant traffic on a channel, the reactive jammer may sense it and attempt to jam it, which offers the opportunity for legitimate traffic on other channels to pass through. On the other hand, the over-increase of traffic will surely decrease the delay performance since transmissions have a high probability to collide with each other. Hence, there should be an optimal traffic load such that the worst-case message delay can be minimized.

Remark 3: In the smart grid, a node's traffic load is usually static and quite unsaturated for monitoring and control on critical power devices. For example, wireless monitoring for substation transformers only needs to transmit a message every second [11]. This indicates that in general, we should intentionally increase a certain amount of redundant traffic to obtain the optimal traffic load. Then, legitimate messages can have a chance to be successfully delivered during the period that jamming attacks attempt to disrupt redundant traffic. We name such traffic as *camouflage traffic* since it serves as camouflage to "hide" legitimate traffic from attacks.

IV. Smart Grid Application: Anti-Islanding

In this section, we use experiments to measure how much gain we can obtain by transmitting camouflage traffic for a smart grid application, anti-islanding, under jamming attacks.

A. Background on Anti-Islanding

Anti-islanding is an important protection procedure for distritbuted energy resources (DES) in the smart grid. In power engineering, islanding [3] refers to the condition in which distributed energy resources continue power supply even though the electric utility is disconnected. Unintentional islanding can

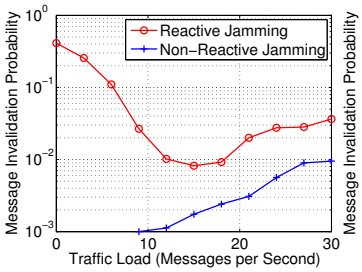

Fig. 2. Message invalidation probability versus traffic load under jamming attacks.

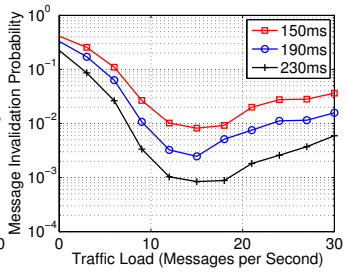

Fig. 3. Performance of message delivery with different delay thresholds under reactive jamming.

cause many problems, such as damaging customers' loads and harming distributed energy resources. Thus, anti-islanding protection procedures must be deployed in power systems to prevent any unintentional islanding.

An anti-island procedure works in the scenario where a load is supplied by both utility and DES: when the utility supply is disconnected, the islanding is detected, an anti-islanding message is sent to the DES to make it stop generating power and prevent potential damages to the DES. The delay threshold of such a message is 150–300ms [3].

B. System Setups

We use universal software radio peripheral (USRP) devices with GNU Radio to set up a frequency-hopping based wireless network to provide jamming resilience for the anti-islanding application. The network consists of five nodes. Each node's routine traffic is one message of status update to the gateway node every second.

There are 8 frequency hopping channels at the 2.4GHz band, each of which uses BPSK modulation and has a bandwidth of 125KHz. The lengths of anti-islanding and camouflage message are 400 and 1000 bytes, respectively. The delay threshold of anti-islanding messages is set to be 150ms.

We also set up a USRP-based jammer with operational bandwidth of 125KHz. When it is non-reactive, it keeps broadcasting jamming pulses, each of which is sent on a randomly selected channel. When it is reactive, it uses an energy detector to scan all 8 hopping channels one by one, and jams any on-going transmission as long as it senses energy activity. The jamming pulse duration is set to be 1ms.

C. Experimental Results

First, we evaluate the impact of both reactive and non-reactive jammers on the anti-island application. We generate camouflage messages at fixed rates of 0–30 messages/second at each IED. Fig. 2 shows that the message invalidation probability for anti-islanding messaging as a function of the camouflage traffic rate of each IED. We can see from Fig. 2 that reactive jamming always leads to worse performance than non-reactive jamming, indicating that we should always consider the reactive jamming as the worst-case scenario. Thus, in the following, we will only consider the reactive jamming. Fig. 2 also shows that the message invalidation probability induced by reactive jamming is a U-shaped function of the traffic load. We can see that the message invalidation probability decreases from 41.2% to 0.82% as the camouflage traffic load goes from 0 to 15 messages/second.

Then, we consider the delay performance with different delay thresholds of 150, 190, and 230ms under reactive jamming. If the delay threshold becomes larger, we can transmit the same message more times to ensure more reliability. Thus, the transmissions have 5, 6, and 7 hops (transmission attempts) for messages with delay thresholds of 150, 190, and 230ms, respectively. Fig. 3 shows that the message invalidation probabilities for different delay thresholds. We can observe that the minimum probabilities are always achieved at 15 messages/second, which in turn indicates that the optimal traffic load is independent of the delay threshold.

Our experimental results show that adequately transmitting camouflage traffic into the network can substantially improve the delay performance under reactive jamming. However, it doesn't help improve the performance in the case of non-reactive jamming. Therefore, in a network with no knowledge of attacks, an appropriate solution is to adaptively generate such traffic to balance the network traffic load at the optimal point, which will be investigated in the journal version.

V. Conclusion

In this paper, we provided a study on minimizing the message delay for smart grid applications under jamming attacks. By defining a generic jamming process, we showed that the worst-case message delay is a U-shaped function of network traffic load. Thus, we show that generating camouflage traffic is a promising method to improve the worst-case delay performance in the smart grid under jamming attacks.

References

[1] NIST Smart Grid Cyber Security Working Group, "Guidelines for smart grid cyber security," *NIST IR-7628*, vol. 1-3, Aug. 2010.

[2] S. Mohagheghi, J. Stoupis, and Z. Wang, "Communication protocols and networks for power systems - current status and future trends," in *Proc. of Power Systems Conference and Exposition*, Mar. 2009.

[3] P. M. Kanabar, M. G. Kanabar, W. El-Khattam, T. S. Sidhu, and A. Shami, "Evaluation of communication technologies for IEC 61850 based distribution automation system with distributed energy resources," in *Proc. of IEEE PES General Meeting*, 2009.

[4] NIST News Release, "Smart grid panel agrees on standards and guidelines for wireless communication, meter upgrades," Apr. 19 2011.

[5] W. Xu, W. Trappe, Y. Zhang, and T. Wood, "The feasibility of launching and detecting jamming attacks in wireless networks," in *Proc. of ACM MobiHoc '05*, 2005, pp. 46–57.

[6] Y. Liu, P. Ning, H. Dai, and A. Liu, "Randomized differential DSSS: Jamming-resistant wireless broadcast communication," in *Proc. of IEEE INFOCOM '10*, Mar. 2010.

[7] M. Strasser, S. Capkun, C. Popper, and M. Cagalj, "Jamming-resistant key establishment using uncoordinated frequency hopping," in *Proc. of IEEE Symposium on Security and Privacy*, May 2008, pp. 64–78.

[8] IEC Standard, "IEC 61850: Communication networks and systems in substations," 2003.

[9] T. S. Sidhu and Y. Yin, "Modelling and simulation for performance evaluation of IEC61850-based substation communication systems," *IEEE Trans. Power Delivery*, vol. 22, no. 3, pp. 1482–1489, July 2007.

[10] F. Cleveland, "Enhancing the reliability and security of the information infrastructure used to manage the power system," in *Proc. of IEEE PES General Meeting*, June 2007.

[11] ——, "Uses of wireless communications to enhance power system reliability," in *Proc. of IEEE PES General Meeting*, June 2007.